Les botmasters

Mythe ou réalité?

David Décary-Hétu

Note de recherche no. 12

Chaire de recherche du Canada en sécurité identité technologie

Université de Montréal

Ce travail a été réalisé dans la cadre du cours CRI-6234, « Nouvelles technologies et crimes » (session d'hiver 2011), offert aux étudiants de la Maîtrise en Criminologie sous la direction du Professeur Benoît Dupont.

La Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal mène des études sur les pratiques délinquantes associées au développement des technologies de l'information, ainsi que sur les mécanismes de contrôle et de régulation permettant d'assurer la sécurité des usagers.

David Décary-Hétu
david.decary-hetu@umontreal.ca

Prof. Benoît Dupont
Centre International de Criminologie Comparée (CICC)
Université de Montréal
CP 6128 Succursale Centre-Ville
Montréal QC H3C 3J7 - Canada
benoit.dupont@umontreal.ca
www.benoitdupont.net
Fax : +1-514-343-2269

Table des matières

Introduction

Le phénomène criminel a vécu de profondes transformations au cours des vingt dernières années. La mondialisation et les innovations dans les transports ont ouvert grand la porte à la création de trafics internationaux de marchandises illicites (Schloenhardt, 1999). Les troubles politiques tant en Europe de l'Est qu'en Afrique ont favorisé le trafic d'armes, la corruption et les marchés noirs (Williams, 1994). S'il est possible d'en connaitre d'avantage si facilement sur ces problématiques, c'est en bonne partie grâce à la démocratisation de l'information amenée par l'internet. Ce médium qui rejoint maintenant une partie appréciable de la population mondiale (Google, 2011) est un puissant outil de communication. L'information y circule à la vitesse de la lumière sans possibilité de la réguler. Ce manque de contrôle a vite été noté par les délinquants qui ont appris à l'utiliser à leur avantage.

Alors que la criminalité informatique se concentrait autour de la fraude, du vol de télécommunication et de la création de code malicieux dans les années 80, elle est aujourd'hui une entreprise diversifiée aux tentacules mondiaux. Certains problèmes ont particulièrement attiré l'attention des médias et du public en général au cours des dernières années.

Nous nous concentrerons au cours de cette recherche sur un type particulier de cyberdélinquance, les botnets. Ces réseaux d'ordinateurs piratés remplissent un rôle de facilitateur de la criminalité informatique. Les aspects techniques de cette criminalité sont aujourd'hui relativement bien étudiés et surveillés, mais on ne peut en dire de même pour ce qui est du côté social. Les individus qui créent et gèrent ces réseaux sont encore très peu connus de la communauté académique et des forces de l'ordre. Ce papier cherchera donc à faire un inventaire des connaissances actuelles sur les botmasters, les individus qui dirigent ces réseaux. La première partie de ce travail exposera comment les botnets en sont venus à jouer un rôle de facilitateur des cybercrimes. La deuxième partie passera en revue la littérature actuelle sur les botnets. La troisième partie identifiera les caractéristiques principales des individus impliqués dans ce type de criminalité. La quatrième et dernière partie classifiera ce type de criminels en fonction de la typologie de Best & Luckenbill (1994). Nous offrirons en guise de conclusions quelques pistes de recherche pour améliorer la collecte de données sur les botmasters.

Les courtiers du crime

Les attaques par déni de service distribué (DDOS[1]) ont fait les manchettes au cours des douze dernières années alors que certains des plus grands sites web ont été rendus inaccessibles par des attaques informatisées (Huffington Post, 2010). Les délinquants à l'origine de ces attaques cherchaient avant tout à se faire connaitre et augmenter leur réputation dans le milieu criminel des pirates informatiques (Mirkovic & al, 2002). C'était le cas entre autres de jeunes comme Mafia Boy, un pirate informatique montréalais condamné depuis à une peine d'emprisonnement pour ses crimes (Calce & al, 2008). Les DDOS ont aujourd'hui une motivation beaucoup plus financière. Les criminels utilisent maintenant leurs ressources pour extorquer des sommes aux entreprises qui dépendent des revenus qu'ils retirent de leurs activités en ligne. Ces dernières doivent se résigner à payer quelques dizaines de milliers de dollars aux délinquants plutôt que perdre des millions en revenus (et une forte baisse de leur réputation). Ce phénomène est particulièrement vrai pour les sites de pari en ligne (McMullan & al, 2007).

Les fraudes de cartes de crédit sont aussi une autre activité en pleine expansion sur internet (Thomas & al, 2006). Les fraudeurs concoctent des stratagèmes de plus en plus ingénieux pour voler des numéros de carte de crédit ainsi que les informations personnelles de leurs détenteurs. Brian Krebs, journaliste américain réputé, présentait récemment la toute dernière invention des fraudeurs : des pièces de rechange de guichets bancaires (Krebs, 2011). En remplaçant les pièces originales par des fausses, les délinquants peuvent recueillir un panier important d'informations sans pour autant alerter les employés ou les clients d'une banque. Il existe aujourd'hui des forums accessibles à tous (ex. : carding.cc) qui permettent aux fraudeurs d'entrer en contact avec des courtiers qui seront en mesure d'utiliser ces informations pour obtenir de l'argent (Thomas & al, 2006). Le développement de tels marchés noirs et surtout le nombre de cartes disponibles sur ces marchés nous montre à quel point l'industrie de la fraude sur internet est rendue lucrative et imposante (Thomas & al, 2006).

Des crimes comme les attaques par déni de service distribué et la fraude de cartes de crédit peuvent sembler être des activités distinctes avec peu de points en commun. La réalité

[1] Les DDOS sont des attaques où le pirate informatique tente de noyer le trafic légitime en direction d'un serveur dans une masse de données afin d'en bloquer l'accès aux utilisateurs légitimes. Dans un tel scénario, un pirate demande à des milliers voire des dizaines de milliers d'ordinateurs sous son contrôle de se connecter simultanément à un serveur. Ne pouvant faire la différence entre une demande légitime de connection et une demande illégitime, le serveur surchargé cessera de répondre à toutes les demandes et deviendra inacessible.

est pourtant toute autre. Il existe en fait un système facilitateur du crime sur l'internet qui permet à ces deux types de crimes, ainsi qu'à plusieurs autres, de se développer et de se maintenir dans le temps. Ce courtier du crime est encore peu connu et nous espérons avec cette recherche permettre aux autres chercheurs ainsi qu'aux services de police d'en connaitre un peu plus sur les individus qui en contrôlent les activités.

Les botnets

Un botnet « réfère à une collection d'ordinateurs compromis (les robots) qui sont contrôlés par un botmaster » (Li & al., 2009 : p.1). Cette définition comporte trois éléments soit les robots, la nation de contrôle et le botmaster. Le botmaster est la personne qui crée et gère le botnet. Son objectif est d'arriver à contrôler le plus grand nombre d'ordinateurs (aussi connus sous le nom de robots ou de zombies). Nous verrons plus tard le type de techniques qui sont utilisées pour arriver à cette fin. Nous retiendrons pour le moment que les outils développés par les botmasters sont extrêmement perfectionnés et les plus grands botnets contrôlent des centaines de milliers d'ordinateurs (Nazario & al, 2008). Le contrôle des botmasters sur les zombies est total; toutes les ressources de l'ordinateur infecté par un botmaster sont à la disposition de celui-ci. Il peut donc autant avoir accès aux données localisées sur le disque dur qu'à la connexion réseau. Les cibles des botmasters sont des plus diverses : il s'agit autant d'ordinateurs personnels que de serveurs d'entreprises (Nazario & al, 2008).

Les botmasters commettent des infractions en deux temps lorsqu'ils s'impliquent dans la gestion de botnets. Ils commettent tout d'abord un crime en prenant le contrôle d'ordinateurs qui ne leur appartiennent pas. Ils commettent ensuite une deuxième série de crime en utilisant ces ordinateurs à des fins criminelles. Cette richesse criminelle pose un problème intéressant aux criminologues, et ce, à plusieurs niveaux.

Tout d'abord, l'impact des botnets sur les réseaux mondiaux est majeur. Nous verrons plus en détail le fonctionnement des botnets, mais comme ceux-ci ont accès aux données enregistrées sur les disques durs des ordinateurs infectés, il leur est possible de siphonner des informations financières personnelles (identifiants, mots de passe, rapports d'impôts) ainsi que des secrets corporatifs. La valeur des données ainsi volées n'a jamais été quantifiée, mais devant l'ampleur des botnets (Nazario & al, 2008), elle ne peut qu'être faramineuse. Les propriétaires des zombies doivent aussi dépenser d'importantes sommes pour se protéger et nettoyer les ordinateurs infectés. Des techniques simples comme l'utilisation d'un routeur ou l'installation de logiciels antivirus offrent une protection relativement bonne et abordable aux

consommateurs, mais les entreprises, universités et autres institutions doivent débourser d'énormes sommes pour se prémunir contre les attaques des botmasters qui tentent de prendre le contrôle de leurs systèmes. Les botnets sont aussi très gourmands en bande passante et peuvent donc augmenter significativement la facture des propriétaires de systèmes infectés.

Les botnets jouent aussi grand rôle de facilitateur dans le monde des cybercrimes. Les botmasters ont deux matières premières très recherchées par les délinquants : des informations et des ressources informatiques. Ces derniers recherchent des informations pour pouvoir en tirer profit (vol d'identité, fraude par carte de crédit, chantage). Ils recherchent également des ressources informatiques pour mener à bien leurs crimes tels l'envoi de pourriel ou encore les attaques distribuées par déni de service. Sans les opérateurs de botnets, ces criminels devraient eux-mêmes parcourir l'internet à la recherche d'informations ou encore programmer des logiciels leur permettant d'attaquer des serveurs web. Les botnets offrent donc un service clé en main à quiconque tente sa chance dans les cybercrimes et se retrouvent donc au cœur de ce que l'on appelle communément les cybercrimes. Ce terme peut d'ailleurs être défini dans son sens le plus large comme « l'utilisation des technologies informatique dans le but de commettre des activités illicites » (Brenner, 2007 : p.13).

La position des botnets dans l'univers des cybercrimes est donc des plus importantes. Nous verrons dans la prochaine section ce que la recherche a pu développer comme connaissances à leur sujet au cours des dernières années ainsi que les lacunes que nous tenterons de combler au travers de cette recherche.

Botmasters et botnets

La littérature sur le sujet des botnets commence à prendre forme avec plus d'une centaine d'articles et de livres recensés sur le sujet. Ceux-ci arrivent maintenant à décrire avec une certaine précision ce que nous pourrions qualifier de script des botnets (Cornish, 1994). Notre revue de littérature suivra ce script du début à la fin et nous permettra de mieux comprendre le fonctionnent d'un botnet.

Afin de bâtir un botnet, deux options s'offrent au botmaster. Il peut tenter de programmer lui-même un logiciel ou encore en acheter un clé en main (Binsalleeh, 2010). La première option est de moins en moins attrayante pour le criminel moyen. Elle nécessite en effet la programmation d'un nombre important de modules ayant chacun une tâche spécifique : 1) exploiter des vulnérabilités (pour prendre le contrôle d'ordinateurs); 2) centre de

communication (pour envoyer des ordres aux zombies); 3) centre de gestion (pour gérer les ordinateurs infectés) et; 4) des vecteurs d'attaques. Produire un logiciel de contrôle de botnet est donc un travail exigeant qui demande des compétences dans plusieurs domaines. Heureusement pour les cybercriminels, ils ont à leur disposition plusieurs logiciels clés en main qui sont mis en vente sur le marché noir (Binsalleeh, 2010). Il existe un nombre important de tels programmes (phpBot, Zeus, SpyBot, Agobot) qui possèdent chacun leurs caractéristiques propres. Leur plus grand avantage est qu'ils permettent d'automatiser la quasi-totalité des tâches qu'un opérateur de botnet doit entreprendre de l'infection d'ordinateurs au contrôle de l'information collectée (Shirley). Certains de ces programmes sont distribués gratuitement alors que les plus performants sont vendus sous forme de licences annuelles qui possèdent des mécanismes de gestion qui empêchent de les copier et ainsi de les installer sur plusieurs ordinateurs à la fois (Binsalleeh, 2010).

Une fois le programme installé, l'opérateur de botnet doit tenter de prendre le contrôle d'ordinateurs et de serveurs vulnérables sur l'internet. Il dispose ici de trois vecteurs d'attaques (Kiran-Kola, 2008). Le premier est l'exploitation de failles de vulnérabilités. Chaque ordinateur infecté tente, à l'aide d'une faille de sécurité, d'exécuter du code malicieux sur un ordinateur auquel il se connecte. Traditionnellement, les zombies vont d'abord tenter d'infecter les machines qui sont sur leur réseau local pour ensuite se tourner vers les machines inconnues sur l'internet. L'opérateur peut spécifier une gamme d'adresses IP spécifiques que chaque machine doit balayer afin de maximiser son rayon d'action. Le botmaster peut aussi utiliser les pièces jointes de courriel pour propager son botnet. Il automatise alors l'envoi de courriel à partir des carnets d'adresses des ordinateurs zombies et joint une copie de son logiciel à chaque courriel envoyé dans l'espoir que le récipiendaire l'ouvre et infecte ainsi son ordinateur. La dernière méthode de transmission est la clé USB. Le logiciel de botnet se copie alors sur toutes les clés USB qui se connectent au zombie et est ainsi transféré d'ordinateur en ordinateur.

À travers ces trois méthodes, l'opérateur de botnet ne cherche qu'à mettre un pied dans de nouveaux systèmes. Une fois cette première étape complétée, le logiciel de botnet installé cherche à télécharger une copie complète du logiciel de contrôle à partir d'un serveur du botmaster (Zhu & al, 2008). Ce logiciel de contrôle indique à l'ordinateur infecté comment recevoir des ordres du botmaster ainsi que comment les exécuter. Le zombie reste alors en veille jusqu'à ce qu'il reçoive les instructions de son maitre. Il existe quatre façons d'établir des

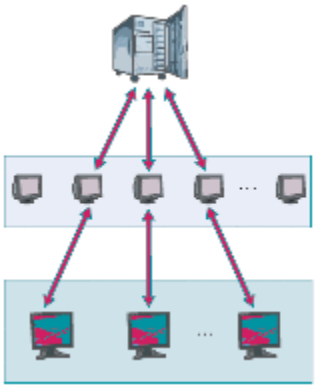
connexions entre un botmaster et un zombie : 1) les chambres IRC; 2) les serveurs HTTP; 3) les réseaux à flux rapide et; 4) les réseaux pairs à pair (P2P).

Les chambres IRC ont été l'outil de prédilection des botmasters pendant de nombreuses années (Zhu & al, 2008), mais sont aujourd'hui de moins en moins utilisées. Ces chambres IRC sont des outils de clavardage sophistiqués qui permettent à des individus d'échange des messages ainsi que des fichiers. Il est possible pour un zombie de se connecter à une chambre IRC et de lire les messages qui s'y échangent. Lorsque le botmaster envoie un ordre, il est alors lu par tous les robots présents dans la salle et ceux-ci s'exécutent alors. Ce type d'infrastructure permet au botmaster de centraliser son centre de commandement et ainsi de communiquer efficacement avec ses robots qui sont toujours en attente d'un ordre (Zhu & al, 2008). Celui-ci peut aussi diviser son armée de zombies en plusieurs sous-groupes qui utilisent chacun des chambres IRC différentes. Ces chambres IRC servent finalement à faire parvenir aux ordinateurs infectés des mises à jour de leur logiciel de contrôle. Ce mode de communication souffre par contre de graves lacunes au niveau de la sécurité. Les services de police et les chercheurs qui arrivent à mettre la main sur une copie du logiciel de contrôle peuvent facilement identifier la chambre IRC à laquelle tous les robots se connectent pour ensuite en prendre le contrôle ou tenter d'identifier la personne qui envoie les ordres. Cette méthode est donc très efficace, mais peu fiable (Zhu & al, 2008).

Afin de jouir d'un plus grand niveau de sécurité, les botmasters ont développé de nouveaux outils leur permettant de communiquer avec leurs zombies à l'aide de serveurs HTTP (Zhu & al, 2008). Au lieu de se connecter à une chambre IRC, les robots cherchent à se connecter à une page web qui contient des instructions ou un lien vers une nouvelle version du logiciel de contrôle. Cette manière de fonctionner permet d'éviter à des inconnus de surveiller les activités du botnet. Il est en effet plus difficile d'épier toutes les connexions à un serveur HTTP afin de compter le nombre d'ordinateurs infectés ainsi que leurs origines. Il est aussi plus facile de changer périodiquement de serveur afin d'éviter tout traçage. Même si cette technique ralentit quelque peu les efforts de détection des forces de l'ordre, il reste qu'une copie du logiciel de contrôle permet de déterminer l'adresse IP du serveur du botmaster. Il est alors possible de le mettre hors service ou dans certains cas, d'en prendre le contrôle à l'aide d'un mandat (Zhu & al, 2008).

L'ingéniosité des botmasters ne s'est pas découragée devant les efforts des chercheurs et des services de police pour les retracer. Ils ont alors décidé d'intégrer à leurs logiciels de contrôle des protocoles de flux rapide.

Figure 1 : Schémas d'un réseau à flux rapide



Dans un tel système, les ordinateurs infectés (bas du diagramme) se connectent à d'autres ordinateurs infectés (rangée du milieu) qui servent à rediriger leurs communications vers le serveur du botmaster (haut du diagramme). Dans un tel système, il est impossible pour les ordinateurs infectés du bas du diagramme de déterminer l'adresse réelle du serveur où sont dirigées leurs communications. Étant donné que les ordinateurs qui servent de relais changent toutes les minutes, il devient extrêmement difficile de retracer le chemin que suivent les messages envoyés par le botmaster. Ce système hautement dynamique pose encore de sérieux problèmes aux chercheurs et aux services de police qui tentent de retracer les responsables qui se cachent derrière les botnets. Étant donné le haut niveau de sophistication requis par ce type d'infrastructure, un nombre très limité de botnets utilise les réseaux à flux rapide, mais ce chiffre est appelé à grandir dans les prochains mois (Nazario, 2008).

Les botmasters peuvent aussi finalement tirer avantage des technologies P2P pour faire transiter leurs messages (Wang & al, 2009). Dans un tel scénario, le botmaster envoie un message à un nombre restreint de zombies qui transmettent à leur tour le message à d'autres zombies et ainsi de suite jusqu'à ce que tous les robots aient reçu les ordres de leur maître. Une telle façon de fonctionner demande plus de temps et un degré relativement élevé de sophistication, mais permet d'éviter les centres de contrôle et de commande. Par ailleurs, même si une partie importante du botnet est éliminée, celui-ci est toujours en mesure de fonctionner (Wang & al, 2009).

Si les botmasters font tant d'effort pour conserver et agrandir leur botnet, c'est avant tout en raison des avantages financiers et personnels que de tels systèmes procurent (Krebs, 2006). Nous reviendrons plus tard aux motivations des individus, mais nous nous devons de noter que ces avantages sont loin d'être négligeables. Les botmasters n'utilisent que rarement leurs botnets à des fins personnelles (Thomas & al, 2006). Ils vont plutôt avoir tendance à retourner sur le marché noir où ils ont acheté leur logiciel de botnet afin de vendre leurs services. Ceux-ci se divisent traditionnellement en six grandes catégories : 1) l'envoi de pourriels; 2) les DDOS; 3) la fraude par clic; 4) l'installation de logiciels publicitaires; 5) l'anonymisation du trafic internet et; 6) le vol d'information.

Les services de courriels ont su développer de puissants filtres afin de détecter rapidement l'origine des pourriels et bloquer tous les messages subséquents. Un botnet permet donc de distribuer la source de campagnes de pourriels sur des milliers d'ordinateurs qui n'envoient alors qu'un petit nombre de pourriels chacun. Cette méthode d'envoi est beaucoup plus discrète et permet de rejoindre un nombre important de cibles sans faire sonner d'alarmes (Banday, 2009). Chaque ordinateur peut aussi recevoir des instructions pour modifier aléatoirement une partie du message afin de rendre les pourriels encore plus difficiles à identifier. Une telle distribution du travail est aussi mortellement efficace dans le cas des DDOS. Dans ce type d'attaque, le botmaster cherche à inonder un ordinateur de requêtes afin qu'il ne soit plus en mesure de répondre aux demandes légitimes de ses utilisateurs. En utilisant des dizaines de milliers d'ordinateurs connectés à l'internet à haut débit, il devient pratiquement impossible de déterminer l'origine de l'attaque qui semble venir des quatre coins de la planète. Même les meilleurs serveurs de la planète ont de la difficulté à survivre à une attaque d'une telle intensité (voir Ars Technica (2010) pour un exemple des attaques du groupe Anonymous sur les serveurs de compagnies de carte de crédit[2]). Les botnets ne servent pas seulement à des fins destructrices comme dans le cas des DDOS. Les botmasters louent aussi leurs réseaux de zombies afin de générer du trafic sur des sites qui reçoivent alors de plus grands revenus publicitaires, un processus mieux connu sous le nom de fraude par clic (Banday, 2009). Les botmasters obtiennent alors une partie des gains supplémentaires ainsi générés. Ces derniers peuvent aussi être rémunérés en échange de l'installation de logiciels publicitaires sur les ordinateurs zombies (Banday, 2009). Ces logiciels vont afficher sur les ordinateurs des personnes infectées des publicités et chaque installation du logiciel permet au botmaster

[2] Certaines compagnies arrivent mieux que d'autres à résister à de telles attaques – voir BBC (2010).

d'obtenir une redevance. Les botmasters peuvent désinstaller puis réinstaller le logiciel plusieurs fois afin de maximiser le rendement de chaque ordinateur infecté. La plus récente innovation des botmasters vient de leur service d'anonymisation du trafic (Krebs, 2011). Ce service permet à des individus de faire transiter leur connexion internet à travers un ou plusieurs ordinateurs infectés. Cela leur permet de camoufler leurs traces ainsi que de modifier leur lieu d'origine. Ce service est extrêmement efficace pour cacher le point d'origine d'une connexion. La dernière fonction des botnets est le vol d'information (Banday, 2009). Tel que mentionné précédemment, les botmasters ont un accès total à l'information enregistrée par l'utilisateur d'un zombie. Ainsi, ses identifiants, ses mots de passe, ses rapports financiers, ses documents de travail sont tous à la portée du botmaster qui peut les voler pour ensuite les revendre au plus offrant sur le marché noir.

Cela n'est pas la première fois que nous parlons de ce «marché noir» des botnets. Il s'agit en fait d'un réseau de forums de discussions et de chambres IRC où diverses activités criminelles se concentrent. Il est possible de s'y procurer le logiciel de contrôle de botnet pour quelques centaines ou quelques milliers de dollars, tout dépendant du type de fonctionnalités requises (Schipka, 2009). Il est aussi possible de louer les services des botnets déjà actifs au même endroit. Les prix demandés sont affichés et les négociations se passent habituellement en messages privés ou par messagerie instantanée (Thomas & al, 2006). Les botmasters recherchent avant tout des clients à long terme afin de réduire les coûts de transaction. Ce marché criminel en vient à devenir une véritable communauté avec sa monnaie virtuelle (des transferts Western Union ou des devises virtuelles comme WebMoney), ses règles et ses coordonnateurs (Thomas & al, 2006). Les administrateurs de ces marchés accordent à tous les participants une cote de fiabilité qui permet à chacun de réduire les chances d'être trompé par l'autre partie d'une transaction[3]. Nous verrons plus tard que ce point central de communication est sûrement le meilleur endroit pour surveiller les botmasters.

Bien que les botnets semblent être des entreprises criminelles faites pour durer (particulièrement celles qui utilisent les réseaux à flux rapide), plusieurs chercheurs ont proposé des techniques pour les attaquer. La première technique consiste à prendre le contrôle des centres de commandes des botnets qu'il s'agisse de chambres IRC ou de serveurs HTTP (Li, 2010). En arrivant à pénétrer dans ces chambres ou ces serveurs, il devient alors possible

[3] Franklin et al. (2007) offrent une bonne discussion des mesures mises en place afin de réduire la fraude sur le marché noir.

d'envoyer l'ordre au logiciel de contrôle de se désinstaller ou encore lui ordonner de se connecter à des serveurs auxquels les botmasters n'ont pas accès. En étant privés de leur lien de communication, les botmasters perdent alors tout contrôle sur leurs zombies. Une telle opération a été menée à terme par Microsoft récemment et à réussit à faire diminuer significativement le nombre de pourriels envoyés sur l'internet (Krebs, 2011). La deuxième technique consiste à produire de l'interférence, et ce, à deux niveaux. Les chercheurs proposent tout d'abord de faire croire au botmaster qu'il contrôle un plus grand nombre de zombies que dans la réalité à l'aide de faux ordinateurs infectés qui ne sont en fait que des machines virtuelles (Li, 2010). Ces machines se connecteraient au centre de contrôle et commande du botmaster, mais ne réagiraient pas aux ordres de ce dernier. En arrivant à infiltrer un botnet avec un nombre relativement large de faux zombies, l'efficacité du botnet en est de beaucoup réduite au point de le rendre peu intéressant aux yeux de clients qui ne peuvent se fier sur les chiffres produits par le botmaster. Celui-ci aura alors plus de difficulté à vendre ses services et cela nuira à ses activités criminelles. L'autre option est de créer de l'interférence sur le marché noir des botnets (Li, 2010). Plusieurs actions peuvent être prises comme la fausse location de service, la fausse proposition de services ou encore la fermeture des forums de discussions qui hébergent ces marchés. En augmentant les coûts de transaction, il devient alors moins rentable pour les botmasters qui devraient logiquement se tourner vers d'autres activités plus lucratives.

La recherche sur les botnets : temps pour un changement de direction

Tel que démontré dans la précédente section, la littérature sur les botnets est relativement imposante dans certains domaines, mais très pauvre dans d'autres. Nous comprenons maintenant relativement bien le fonctionnement technique des botnets ainsi que le script criminel qui s'y rattache. Les botmasters achètent un logiciel sur le marché noir et tentent d'infecter le plus grand nombre possible de machines. Une fois qu'ils ont atteint un certain niveau d'infection, il leur est alors possible de louer leurs machines infectées afin de remplir l'un des six mandats que nous avons décrit ci-dessus. Bien qu'encore élémentaires, quelques techniques de neutralisation ont été suggérées, mais il reste à les mettre en application. La surveillance des botnets ne pose pas elle non plus énormément de problèmes. Des sites comme *Zeus Tracker* ou *Shadowserver Foundation* offrent des décomptes quotidiens

de la taille et de la localisation des botnets actifs partout sur la planète. Nous apprenons ainsi que le botnet de type Zeus est actif sur plus de 500 serveurs sur les cinq continents (avec une forte concentration aux États-Unis et en Europe). Étant donné que la plupart des botnets utilisent toujours des chambres IRC ainsi que des serveurs HTTP pour communiquer, leur surveillance est relativement aisée une fois que les chercheurs ont réussi à capturer une copie du logiciel qui se propage sur l'internet.

Avec tant d'informations disponibles, la question se pose à savoir pourquoi ce type de crime, un des grands facilitateurs de la cybercriminalité, est toujours aussi problématique à ce jour. En effet, plusieurs botnets ont été mis hors d'état de nuire au cours des dernières sans pour autant diminuer significativement le nombre de machines infectées. Une étude récente notait d'ailleurs qu'une bonne partie des 1000 plus grandes compagnies américaines étaient infestées par des botnets (Krebs, 2010). Étant donné nos connaissances étendues de l'aspect technique du problème, nous devons nous tourner vers l'aspect social des botnets. En effet, les études que nous avons présentées jusqu'à maintenant se concentrent particulièrement sur les botnets et mentionnent régulièrement les botmasters sans leur donner la place qu'ils méritent. Toutes ces recherches partent avec la prémisse que quelqu'un, quelque part, contrôle des dizaines de milliers d'ordinateurs zombies, mais presque aucune d'entre elles ne fait l'effort de tenter de comprendre qui se cache derrière ce terme de botmasters. Ces derniers semblent exister et ce simple fait contente la communauté scientifique[4].

Notre position est que les botmasters ne sont pas que des êtres mystérieux qui devraient être une arrière-pensée des devis de recherche, mais bien le centre de l'attention des communautés scientifiques. Si nous continuons à nous intéresser à la technologie des botnets, nous serons éternellement une étape derrière ceux qui la développent. Afin de pouvoir avoir un impact sur le phénomène des botnets, il devient de plus en plus urgent d'amasser un savoir cohérent à leur sujet si nous voulons les comprendre et bâtir une régulation sociale efficace. Comme nous l'avons démontré au début de ce papier, les opérateurs de botnets sont des facilitateurs de plusieurs types de crimes (DDOS, pourriels, fraudes, anonymisation, vols d'informations). En réussissant à mieux comprendre leurs profils sociodémographiques, leurs motivations, leurs relations les uns avec les autres, nous serons en mesure de mieux les détecter et de mieux les contrôler.

[4] D'autres pourraient argumenter à l'effet que les chercheurs ne disposent pas des outils nécessaires à l'étude de la dimension sociale. La présente étude se veut la preuve de la non-recevabilité d'un tel argument.

Cette recherche a donc pour objectif principal de dresser un portait des opérateurs de botnets. Pour ce faire, nous utiliserons les sources citées dans notre revue de littérature ci-dessus. Les informations relatives aux botmasters sont souvent implicites et notre tâche sera donc de les faire ressortir au grand jour et de les compiler dans un tout cohérent. Nous utiliserons aussi certaines sources journalistiques reconnues afin de bonifier les informations déjà connues. Certains articles produits par le sujet par des journalistes comme Brian Krebs (anciennement du Washington Post) offrent un produit sérieux et rigoureux qui n'a que très peu à envier aux recherches dans le domaine.

Notre portrait des opérateurs de botnets se divisera en cinq catégories : 1) profil sociodémographique; 2) profil psychologique; 3) motivation; 4) relations personnelles et professionnelles et; 5) capacité technique. Nous espérons ainsi dresser un portrait aussi complet que possible de ce type de criminel dans un cadre descriptif. Nos données seront par la suite analysées à la lumière de la classification des caractéristiques de l'organisation de sous-cultures déviantes de Best et Luckenbill (1994). Ce cadre théorique affirme qu'il existe quatre niveaux dans la sophistication des groupes déviants. Les solitaires sont le plus élémentaires de tous et s'associent très peu les uns avec les autres. Ils ne vont que rarement commettre des délits avec d'autres codélinquants. Les collègues créent une sous-culture déviante et partagent un certain savoir commun. Il n'existe ici encore que peu de cas de codélinquance et aucune division du travail. Les pairs ont toutes les caractéristiques des collègues, mais commettent des crimes avec d'autres individus. Ces associations sont élémentaires et ne durent pas dans le temps. Finalement, les équipes forment la catégorie la plus sophistiquée. Leurs associations de criminels sont plus stables dans le temps et se partagent les tâches afin de maximiser leur efficacité criminelle. Nous pourrons, à la lumière de ce cadre théorique, mieux définir le niveau de sophistication des botmasters et ainsi mieux identifier la menace qu'ils posent et les meilleurs moyens de les réguler.

Les botmasters

Le profil sociodémographique

Nous avons très peu de connaissances sur le profil sociodémographique des opérateurs de botnet. Les seules données disponibles proviennent des écrits de journalistes qui ont interviewé des botmasters (Krebs, 2010). Il ressort de ces recherches qu'ils sont des hommes

âgés entre 19 et 31 ans. Ils n'ont pas d'origine spécifique venant d'Europe comme des États-Unis. Leur niveau scolaire est relativement bas avec certains individus qui ont fréquenté l'université sans la terminer alors que d'autres n'ont même pas terminé leur secondaire. Il semble surtout s'agir de caucasiens qui contrôlent en moyenne quelques dizaines de milliers de zombies dans leurs botnets.

Plusieurs d'entre eux gagnent d'importantes sommes d'argent (Krebs, 2010). Tout dépendant de la source mentionnée, les botmasters peuvent se faire de quelques milliers à quelques dizaines de milliers de dollars par mois pour un nombre très limité d'heures de travail. Selon les recherches, un botnet se loue en moyenne 0.04$/robot et les botmasters reçoivent entre 0.05$ et 0.25$ par logiciel publicitaire qu'ils installent. Selon une firme qui offre de rémunérer pour l'installation de logiciels publicitaires, un botnet de 5000 robots peut générer jusqu'à 22 000$ de revenus par mois.

Les botmasters n'ont pas à investir un nombre d'heures très important pour gérer leur botnet qui est la plupart du temps sur ce que l'on pourrait qualifier d'autopilote (Krebs, 2010). Aucun auteur ne s'est intéressé jusqu'à maintenant au nombre d'heures requis afin de bâtir un botnet à proprement parlé. Il devient donc difficile d'établir des comparaisons entre ces pirates et d'autres catégories de cybercriminels. Les lacunes dans ce domaine sont donc importantes et de nouvelles techniques devront être utilisées pour combler ce déficit dans les connaissances.

Le profil psychologique

Il existe aussi très peu de données sur le profil psychologique des botmasters. Un article relate les doutes et le sentiment de culpabilité qu'éprouve un botmaster face à ses actions. Il comprend qu'il commet des crimes qui pourraient l'envoyer en prison et éprouve du stress et des remords. L'article nous apprend que ces sentiments auront raison de ses activités illicites. Ce cas est possiblement différent des autres, car il relate les problèmes d'un individu plus jeune qui vit toujours chez ses parents malgré les revenus importants qu'il reçoit.

D'autres botmasters un peu plus âgés font preuve de pensée magique ainsi qu'une grande impulsivité. Ils ont aussi de la difficulté à vivre avec les délais et les refus. L'auteur relate ici le cas de trois opérateurs de botnet espagnols, qui, une fois arrêtés, ont tenté de se faire embaucher par la compagnie de sécurité informatique qui les avait démasqués. Ils espéraient que leur expérience criminelle ferait d'eux des employés intéressants pour la compagnie. Ils étaient très pressés de passer au travers du processus d'embauche étant donné leur situation précaire. Nous pouvons donc supposer que ces derniers dilapidaient leurs revenus aussi

rapidement qu'ils ne le gagnaient. Lorsqu'ils se sont finalement refusé un emploi, les botmasters ont alors menacé de divulguer des failles de sécurité et de s'attaquer à la compagnie en question – une attitude plus proche d'un enfant boudeur que de celle d'un grand délinquant antisocial.

En étudiant la littérature, nous pouvons identifier certains autres traits en lien avec le profil psychologique des botmasters. Ce sont tout d'abord des individus qui ont un sens de la toute-puissance et de l'invincibilité. Plusieurs chercheurs affirment que les forums où se transigent les informations et les services des botnets sont ouverts à tous. Les botmasters n'hésitent pas à y afficher leurs courriels ou encore leur compte de messagerie instantanée ainsi que les services qu'ils sont prêts à offrir. Cela revient à offrir une piste aux enquêteurs ainsi qu'une liste de leurs délits. Ils affirment donc qu'ils n'ont que peu de crainte de se faire arrêter et ce sentiment est potentiellement renforcé par le faible nombre d'arrestations d'opérateurs de botnets ainsi que le fait que plusieurs juridictions ne reconnaissent toujours pas cette activité comme un crime (comme en Espagne par exemple).

Les botmasters font aussi preuve d'un faible sens éthique à deux niveaux. Tout d'abord, ils commettent des infractions criminelles diversifiées sur une certaine période de temps. Bâtir un botnet ne se réalise pas en quelques minutes et comme nous l'avons mentionné ci-dessus, il est nécessaire d'investir dans un logiciel de contrôle ou à tout le moins de faire des recherches pour en télécharger un. Cela demande un investissement dans une délinquance organisée qui réfère à un sens éthique relativement faible. Par ailleurs, les botmasters évoluent dans un milieu peu structuré et peu régulé. Ils doivent pourtant négocier et interagir avec les partenaires qui leur vendent les logiciels de contrôle ainsi que les personnes qui louent leurs services. Il arrive constamment que les ententes ne soient pas respectées par l'une ou l'autre des parties (Thomas & al, 2006). Dans ce contexte, le sens moral, sans aucune surprise, doit être considéré comme faible chez les botmasters.

La motivation

La motivation des botmasters semble être l'argent. Toutes les études concordent d'ailleurs sur ce sujet : l'objectif de tout botmaster est de faire le maximum de gains. Cela est représentatif de la diversité des activités des botnets. Étant donné le nombre grandissant de botnets actifs, les botmasters doivent encore et toujours trouver de nouvelles activités pour se démarquer et offrir un produit plus compétitif. C'est pour cette raison que nous avons vu récemment l'apparition de services d'anonymisation de trafic, service qui n'était pas cité comme

une activité des botmasters encore tout récemment. Étant donné les sommes importantes que les botnets génèrent, il n'est guère étonnant de voir les botmasters investir autant dans la recherche de nouveaux ordinateurs à contrôler.

De manière surprenante, les études ne font pas de cas de la réputation comme étant un élément important chez les botmasters. Plusieurs autres types de criminalité informatique comme la scène des warez (Rehn, 2003) considèrent que la réputation et la valeur d'un pirate sont les choses les plus importantes. Nous n'avons pas été en mesure de constater l'impact d'un tel combat chez les opérateurs de botnets. Le côté affaire des botnets aurait donc pris entièrement le dessus sur de vaines querelles d'ego.

Les relations personnelles et professionnelles

Plusieurs recherchent affirment que les botmasters convergent vers des lieux centraux (Thomas & al, 2006). Ces forums de discussions et chambres IRC sont des lieux où les délinquants peuvent partager leurs expériences et tenter d'améliorer leurs capacités. Il s'agit donc ici de relations positives dans l'ensemble. Il existe bien quelques dissensions et conflits entre les participants, mais en général le sentiment d'appartenir à une communauté fermée l'emporte sur les querelles.

Toutes les relations entre botmasters ne sont cependant pas dans un mode aussi transparent. Les opérateurs de botnets se livrent en effet des guerres qui visent à subtiliser les botnets des adversaires (Friess, 2007). En prenant le contrôle de la chambre IRC d'autres botmasters, un délinquant peut facilement augmenter de plusieurs dizaines de milliers de zombies sont propre réseau. Les versions les plus récentes des logiciels de contrôle tentent donc d'effacer toutes traces d'autres logiciels de botnet avant de s'installer. Les plus grands opérateurs sont aussi constamment à la recherche de centres de contrôle vulnérables afin d'augmenter rapidement et avec peu d'efforts leurs réseaux. Tous les coups sont ainsi permis et certaines alliances temporaires peuvent se créer afin de renforcer temporairement un réseau contre les attaques.

Les botmasters doivent aussi composer avec des partenaires d'affaires qui ne veulent pas toujours leur bien. Étant donné le manque de régulation du monde interlope, les botmasters doivent faire confiance aux individus qui louent leurs services. Les paiements manquent souvent et la confiance est dure à établir (Stone-Gross, 2011). Les vols de services sont courants tout comme les défauts de paiement.

L'univers des botnets est donc un environnement hostile pour les botmasters qui doivent se méfier non seulement des forces de l'ordre, mais aussi des autres participants de leurs communautés. Un tel contexte ne peut être que générateur d'une grande quantité de stress et de tension interne. Par ailleurs, les botmasters ne disposent d'aucun revenu garantit. Cex deux facteurs pourraient expliquer pourquoi on ne retrouve que de jeunes opérateurs de botnets, les plus vieux prenant leur retraite à un âge relativement jeune.

Les capacités techniques

Les chercheurs s'entendent pour dire que la majorité des botmasters n'ont que de faibles capacités techniques (Fucs & al). Ils n'ont en effet pas vraiment d'éducation formelle comme nous l'avons. Un chercheur relate que les opérateurs savent programmer (Krebs, 2006) et même que l'un deux s'est lancé dans le domaine à l'âge précoce de 14 ans. La plupart d'entre eux utilisent par contre des logiciels de contrôle clé en main et les recherchent prouvent qu'ils ne sont pas en mesure de modifier le code source qu'ils achètent. Il s'agit donc surtout de jeunes qui maximisent leur potentiel criminel en utilisant les outils disponibles. Il serait donc intéressant de s'intéresser dans des recherches futures aux personnes qui programment les logiciels de contrôle et qui permettent ainsi aux masses de botmasters de se lancer dans la vie délinquante. Il est par contre possiblement trop tard pour faire disparaitre ces logiciels de contrôle de l'internet. Une fois distribuée, une information ne peut disparaitre totalement de l'internet.

Il est important de noter que, malgré leurs capacités limitées, les botmasters sont d'ordinaire assez prudents. Ils savent qu'il est nécessaire de crypter ses communications et d'utiliser des services d'anonymisation du trafic afin de camoufler ses traces. Certains vont relâcher leur garde quelques instants et seront alors rapidement identifiés (Krebs, 2010), mais leurs capacités limitées à programmer ne devraient pas faire oublier qu'ils disposent d'une bonne connaissance du fonctionnement de l'internet et qu'ils discutent entre eux des meilleurs moyens de protéger leur identité.

Les botmasters : solitaires, pairs, collègues ou équipes?

La section précédente nous a permis de faire l'inventaire des connaissances actuelles sur les botmasters. Il ressort de cette analyse que les botmasters pourraient être classifiés comme

des équipes selon la typologie de Best et Luckenbill (1994). Nous avons donc affaire ici au niveau le plus développé de la délinquance.

Il existe en effet une division claire du travail entre ceux qui produisent les logiciels, ceux qui les utilisent et ceux qui profitent des données ainsi recueillies. La collaboration entre ces différents groupes est déjà bien cimentée et les contacts sont facilités par des chambres IRC et des forums de discussion en ligne qui permettent à tous de vendre et d'acheter des services en plus de demander de l'aide. Le fait que ces individus se spécialisent dans l'une ou l'autre des activités permet aussi de croire qu'ils ont atteint un certain niveau de sophistication et d'efficacité qui donne peu de chances aux services de police qui tente de les contrôler.

La construction d'un botnet demandant un certain investissement dans le temps, ces structures auront tendance à survivre pendant une certaine période de temps. Plusieurs sites offrent la possibilité de suivre l'évolution des différents botnets (ZeusTracker, ShadowServer Foundation). Les données issues de ces sites viennent confirmer cette affirmation. Tel que mentionné plus tôt dans le texte, les criminels recherchent avant tout des clients stables afin de minimiser les coûts de transaction.

Au niveau technologique, les botmasters peuvnet maintenant compter sur des logiciels malveillants à la fine pointe de la technologie qui permettent d'encrypter les données transférées, d'utiliser des proxy et de cibler les informations collectées sur chaque ordinateur infecté. Une fois lancé sur Internet, ces logiciels malveillants infectent continuellement de nouveaux systèmes sans intervention du botmaster qui peut alors se concentrer sur la gestion de son poste de commandement.

Le constat que nous posons ici devrait être un signal d'alarme pour les services de police qui s'intéressent au problème. Devant un tel degré de sophistication, ces derniers devront investir d'importantes ressources si elles veulent résussir à endiguer le flot de zombies qui grossit sur une base quotidienne. Les botnets sont maintenant sous le contrôle d'un crime organisé et l'approche des policiers devra tenir compte de ce fait. Des arrestations aléatoires ne seront ici que de peu d'utilité. Les joueurs stratégiques devraient plutôt être identifiés par les services de l'ordre afin de maximiser l'impact des ressources investies. Nous avons démontré dans ce travail comment les botmasters dépendaient des producteurs de logiciels malveillants. Cette catégorie de pirates nous semble être une cible prioritaire afin de tarir le flot de nouveaux logiciels toujours plus sophistiqués. Les enquêtes subséquentes pourraient par la suite se concentrer sur les botmasters notamment en s'attaquant aux revenus illicites qu'ils retirent de

la location de leurs botnets. Ce n'est qu'en adoptant une stratégie d'intervention conséquente que les services de l'ordre pourront véritablement avoir un impact sur la communauté des botnets.

Les opérateurs de botnets et leurs codélinquants forment maintenant une communauté mature similaire à celle du piratage de propriété intellectuelle (Rehn, 2003). Nous verrons dans la conclusion que les limites du contrôle social les visant peuvent être contournées et qu'il est toujours possible de trouver une faille permettant d'amasser des données à leur sujet.

Conclusion

Les cybercrimes sont une problématique qui attire de plus en plus le regard des chercheurs et des journalistes. Ce papier se voulait une première incursion dans le monde encore peu connu des botmasters. Nous avons été en mesure de constater le faible niveau de connaissances disponibles à leur sujet. Malgré cette limite, les éléments actuels de connaissance semblent indiquer que les botmasters sont surtout de jeunes hommes peu éduqués qui arrivent à amasser des sommes importantes à travers leurs activités criminelles. Ils ont un faible sens de l'éthique, sont capables d'éprouver des remords et font preuve d'une certaine impulsivité. Ils sont motivés par l'argent et évoluent dans un environnement hostile où les alliances se font et se défont. Ils peuvent obtenir de l'aide auprès de certains de leurs collègues, mais doivent toujours se méfier d'autres botmasters qui voudraient voler leurs zombies. Ils possèdent des capacités techniques limitées, mais cela ne les empêche pas de bâtir des botnets comprenant plusieurs dizaines de milliers de robots.

Nous pensons qu'il est urgent que les chercheurs concentrent leur attention sur ces individus plutôt que sur les réseaux qu'ils bâtissent. Pour chaque botnet qui est mis hors d'état, deux autres repoussent étant donné que les botmasters ne sont jamais arrêtés et qu'ils conservent toujours une copie de leur logiciel de contrôle ce qui leur permet de repartir à neuf même si leur botnet est complètement démantelé. Afin d'arriver à amasser plus de connaissances sur ces individus, nous proposons une approche en deux temps.

Les chercheurs peuvent d'ores et déjà accéder au marché noir sur lequel évoluent ces pirates. Il devient alors très aisé de faire une copie de toutes les discussions publiques des botmasters et ainsi de tenter d'en apprendre plus sur leurs profils et leurs caractéristiques. Des outils permettent d'automatiser le processus (Web Scraper+ par exemple) et il est aussi possible d'enregistrer automatiquement toutes les conversations d'une chambre IRC en particulier. Ces

lieux de convergence des pirates pourraient aussi permettre aux chercheurs d'entrer en contact avec les botmasters eux-mêmes afin de tenter d'en apprendre davantage sur eux. Les criminels répondent habituellement bien à de telles aventures (Taylor, 1999) et la technique pourrait être ici des plus utiles pour bâtir une ethnographie de la communauté des botmasters.

Les chercheurs pourraient aussi tirer des données intéressantes des quelques dossiers d'enquêtes policières qui ont visé des botmasters. Bien que rares, ces enquêtes sont souvent des sources importantes de données qui comprennent des quantités impressionnantes de journaux de clavardage riches en informations. Les policiers ont aussi la capacité de dresser des portraits exhaustifs des individus impliqués et donc de fournir un profil complet des botmasters.

Bien qu'importants, les botmasters ne doivent pas devenir le seul centre d'attention des chercheurs. Les développements technologiques sont rapides dans le domaine des botnets et il sera important de maintenir nos connaissances à jour. Au cours des derniers mois, nous avons été témoin de la création d'un nouveau type de botnet qui utilise les téléphones cellulaires Android plutôt que des ordinateurs comme hôte. Cette innovation ouvre un nouveau champ d'application pour les botmasters et de tels développements nous rappellent à quel point de grands efforts seront nécessaires afin de comprendre le phénomène des botnets au cours des prochaines années.

Avec leur rôle de facilitateur, les botnets offrent une cible de choix à quiconque voudrait en apprendre plus sur les cybercrimes et tenter de réguler cette criminalité. La connaissance est ici, comme sur l'internet, la clé du succès. Cette recherche est un premier pas dans la bonne direction et nous espérons que les pistes lancées ici permettront à d'autres de porter encore plus loin le flambeau des connaissances.

Références

Alexander K. Seewald, W. N. G. (2010). "On the detection and identification of botnets." *Computers And Security* 29: 45-58.

Alper Caglayan, M. T., Dan Drapeau, Dustin Burke and Gerry Eaton (2009). "Real-Time Detection of Fast Flux Service Networks". *Cybersecurity Applications & Technology Conference For Homeland Security*.

Anderson, N. (2007). "Vint Cerf: One Quarter Of All Computers Part Of A Botnet". *Ars Technica*.

Ard, C. (2007). "Botnet Analysis." *International Journal Of Forensic Computer Science* 1: 65-74.

Banday, M. T., Qadri, J.A., Shah, N.A. (2009). "Study Of Botnets And Their Threats To Internet Security." *Sprouts: Working Papers On Information Systems* 9(24): 2-12.

Barroso, D. (2007). "Botnets – The Silent Threat". *European Network And Information Security Agency*.

BBC (2010). "Pro-Wikileaks activists abandon Amazon cyber attack". Récupéré au: http://www.bbc.co.uk/news/technology-11957367.

Best, J., Luckenbill, D. (1994). "Organizing Deviance, 2nd edition". New Jersey: Prentice Hall.

Corbin, J., and A. Strauss. (I990). "Grounded theory research: Procedures, canons, and evaluative criteria". *Qualitative Sociology* 13 (1): 3-21.

Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., Wang, L. (2010). "On The Analysis Of The Zeus Botnet Crimeware Toolkit". *Privacy Security And Trust*. Ottawa, Ontario, p.31-p.38.

Bleaken, D. (2010). "Botwars: The Fight Against Criminal Cyber Networks". Récupéré au: http://www.symantec.com/connect/blogs/botwars-fight-against-criminal-cyber-networks.

Bosker, B. (2010).). "Visa DOWN: WikiLeaks Suporters Take Down Site As Payback". Récupéré au : http://www.huffingtonpost.com/2010/12/08/visa-down-wikileaks-suppo_n_794039.html.

Brent ByungHoon Kang, E. C.-T., Christopher P. Lee, James Tyra, Hun Jeong Kang, Chris Nunnery, Zachariah Wadler, Greg Sinclair, Nicholas Hopper, David Dagon, Yongdae Kim (2009). "Towards Complete Node Enumeration in a Peer-to-Peer Botnet". *ASIACCS*. Sydney, Australie.

Calce, M., Silverman, C. (2008). "Mafiaboy : How I Cracked The Internet And Why It's Still Broken". Viking: Canada, Ontario.

Carlton R. Davis, S. N., Josee M. Fernandez, Jean-Marc Robert, John McHugh (2008). "Structured Peer-to-Peer Overlay Networks: Ideal Botnets Command and Control Infrastructures?" *Computer Science* 5283: 461-480.

CERT (16 août 2010). "CERT-FI Advisory on the Outpost24 TCP Issues". Récupéré au : https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html.

Christian Rossow, C. D., Dr Norbert Pohlmann (2009). "Botnets - Litterature Survey And Report". *Ministère de l'Innovation de l'Allemagne*.

Cornish, D. (1994). "The Procedural Analysis Of Offending And Its Relevence For Situational Prevention". *Crime Prevention Studies* 3 p151-p196.

D. Dagon, C. Zou, andW. Lee (2006). "Modeling botnet propagation using time zones". *13th Network and Distributed System Security Symposium* (NDSS).

Fogie, S. (20 décembre 2002). "Close Encounters Of The Hacker Kind: A Story From The Front Line". *InformIT*.

Franklin, J., Perrig, A., Paxson, V. Savage, S (2007). "An Inquiry Into The Nature And Causes Of The Wealth Of Internet Miscreants". *Conference On Computer And Communications Security*.

F. Freiling, T. Holz, and G. Wicherski (2005). "Botnet tracking: Exploring a root cause methodology to preventing denial-of-service attacks". *10th European Symposium on Research in Computer Security* (ESORICS).

Fucs, A., de Barros, p., Pereira, P. "New botnets trends and threats". Récupéré au : http://www.blackhat.com/presentations/bh-europe-07/Fucs-Paes-de-Barros-Pereira/Whitepaper/bh-eu-07-barros-WP.pdf

Google (2011). "Statistiques d'utilisation d'internet". Récupéré au : http://www.google.com/publicdata?ds=wb-wdi&met=it_net_user_p2&idim=country:CAN&dl=en&hl=en&q=internet+usage#met=it_net_user_p2&idim=country:CAN&tdim=true

Higgins, K. J. (2007). "The World's Biggest Botnets."

Hudson, S. (2007). "An Analysis Of Botnet Vulnerabilities". *Department Of The Air Force*, Air Force Institute Of Technology.

Joan Calvet, C. R. D., Pierre-Marc Bureau (2009). "Malware Authors Don't Learn, and That's Good! ". *4th International Conference On Malicious and Unwanted Software*. Montreal, Canada: 88-97.

Jose Nazario, T. H. (2008). "As the Net Churns: Fast-Flux Botnet Observations". *3rd International Conference on Malicious and Unwanted Software*. Fairfax, USA.

Katsumi Ono, I. K., Toshihiko Kamon (2007). "Trend of Botnet Activities". *41st Annual IEEE International Carnahan Conference On Security Technology*. Ottawa, Canada: 243-249.

Ken Dunham, J. M. (2008). "Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet". Auerbach Publications.

Krebs, B. (16 août 2005). "Adware Firm Accuses 7 Distributors Of Using Botnets". Washington Post.

Krebs, B. (19 février 2006). "Invasion Of The Computer Snatchers". Washington Post.

Krebs, B. (21 mars 2006). "Bringing Botnets Out Of The Shadows". Washington Post.

Krebs, B. (Mai 2010). "Accused Mariposa Botnet Operators Sought Jobs At Spanish Security Firm". Récupéré au: http://krebsonsecurity.com/2010/05/accused-mariposa-botnet-operators-sought-jobs-at-spanish-security-firm/.

Krebs, B. (28 juillet 2010). "Alleged Mariposa Botnet Author Nabbed". Récupéré au: http://krebsonsecurity.com/2010/07/alleged-mariposa-botnet-author-nabbed/.

Krebs, B. (11 avril 2011). "Is Your Computer Listed For Rent? ". Récupéré au: http://krebsonsecurity.com/2011/04/is-your-computer-listed-for-rent/

McMullan. J, Perrier, D. (2007). "The Security Of Gambling And Gambling With Security: Hacking, Law Enforcement And Public Policy". *International Gambling Studies* 7:1, p.43-p.58.

Mirkovic, J. (2004). "A Taxonomy Of DDOS Attack And DDOS Defense Mechanisms". *ACM SIGCOMM Computer Communication Review*, 34:2.

Nazario, D. J. (2006). "Botnets – The Silent Threat". *Virus Bulletin*. Montreal, Canada.

Nazariom D.J. (2008). "DDOS Attack Evolution". *Network Security*, 2008:7, p.7-p.10.

Nevena Vratonjic, M. H. M., Maxim Raya, Jean-Pierre Hubaux. "ISPs and Ad Networks Against Botnet Ad Fraud."

Paul Craig, M. B. (2005). "Software Piracy Exposed". Rockalnd, MA, Syngress.

Pavel Celeda, R. K., Jan Vykopal, Martin Drasar (2010). "Embedded Malware – An Analysis of the Chuck Norris Botnet". *European Conference On Computer Network Defense*.

Phifer, L. (18 février 2011). "The Top 10 Botnet Events Of 2010". *eSecurity Planet*.

Prince, B. (16 février 2011). "RSA Conference: Researchers Go Inside the Botnet Threat". *eWeek.com*.

M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis (2006). "A multifaceted approach to understanding the botnet phenomenon". *IMC*.

Rehn, A. (2003). "The politics of contraband: The honor economies of the warez scene." *Journal of Socio-Economics* 33: 359-374.

Rogers, M. (2000). "A New Taxonomy".

Sabourin, C. (17 février 2011). "Des ministères canadiens visés par une cyberattaque venant de Chine." Récupéré au : http://technaute.cyberpresse.ca/nouvelles/internet/201102/17/01-4371202-des-ministeres-canadiens-vises-par-une-cyberattaque-venant-de-chine.php.

Saikat Guha, P. F. (2007). "Identity Trail: Covert Surveillance Using DNS". *7th International Conference On Privacy Enhancing Technologies*.

Sandeep Yadav, A. K. K. R., A.L. Narasimha Reddy, Supranamaya Ranjan (2010). "Detecting Algorithmically Generated Malicious Domain Names". *ICM*. Melbourne, Australie.

Schultz, E. (2006). "Where Have The Worms And Viruses Gone? New Trends In Malware." *Computer Fraud & Security*(7): 4-8.

Shirley, B. "Botnet Literature Review."

Taylor, P. (1999). "Hackers: Crime In The Digital Sublime". New York: Routledge.

Thomas, R., Martin, J. (2006). "The Underground Economy: Priceless". *Login*, 31:6.

R. Vogt, J. Aycock, M. J. Jacobson, and Jr (2007). "Army of botnets". *NDSS*.

P. Wang, S. Sparks, and C. C. Zou (2007). "An advanced hybrid peer-to-peer botnet". *First Workshop on Hot Topics in Understanding Botnets*. University of Central Florida.

West, M. (2008). "Threats That Computer Botnets Pose to International Businesses". *Department of Business*, Youville College: 69.

Zhaosheng Zhu, G. L., Yan Chen, Zhi Judy Fu, Phil Roberts, Keesook Han (2008). "Botnet Research Survey". *Annual IEEE International Computer Software and Applications Conference*.

Zhen Li, Q. L., Aaron Striegel (2009). "Botnet Economics: Uncertainty Matters." *Managing Information Risk And The Economics Of Security*: 245-267.

Zhen Li, Q. L., Andrew Blaich, Aaron Striegel and 2 (2010). "Fighting botnets with economic uncertainty." *Security And Communication Networks*.